Amendments to the Claims

1-2. (canceled)

3. (previously presented) The cryptography engine of claim 68, wherein the cryptography engine is a DES engine.

4. (canceled)

5. (currently amended) The cryptography engine of claim 71, wherein the [[second]] third bit sequence is less than 32 bits.

6. (currently amended) The cryptography engine of claim 71, wherein the [[second]] third bit sequence is four bits.

7. (previously presented) The cryptography engine of claim 5, wherein the first bit sequence is less than 48 bits.

8 . (previously presented) The cryptography engine of claim 6, wherein the first bit sequence is less than six bits.

9-10. (canceled)

11. (currently amended) The cryptography engine of claim 68, wherein the [[combined]] fourth bit sequence is less than 32 bits.

12. (currently amended) The cryptography engine of claim 68, wherein the [[combined]] fourth bit sequence is four bits.

13. (previously presented) The cryptography engine of claim 68, further comprising a multiplexer circuitry including a two-level multiplexer.

14. (previously presented) The cryptography engine of claim 13, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer.

15. (canceled)

16. (previously presented) The cryptography engine of claim 68, wherein the key scheduler performs pipelined key scheduling logic.

17. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a determination stage.

18. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a shift stage.

19. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a propagation stage.

20. (previously presented) The cryptography engine of claim 68, wherein the key scheduler comprises a consumption stage.

21. (previously presented) The cryptography engine of claim 17, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

22-45. (canceled)

46. (currently amended) The integrated circuit layout of claim 73, wherein the cryptography engine [[in]] is a DES engine.

47. (canceled)

48. (previously presented) The integrated circuit layout of claim 76, wherein the first bit sequence is four bits.

49. (previously presented) The integrated circuit layout of claim 48, wherein the expanded first bit sequence is less than six bits.

50. (previously presented) The integrated circuit layout of claim 73, wherein the key scheduler performs pipelined key scheduling logic.

51. (previously presented) The integrated circuit layout of claim 73, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

52. (previously presented) The integrated circuit layout of claim 51, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

53. (previously presented) The integrated circuit layout of claim 73, further comprising a multiplexer circuitry including a two-level multiplexer.

54. (previously presented) The integrated circuit layout of claim 53, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to an output stage of the multiplexer.

55-67. (canceled)

68. (currently amended) A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

means for combining via a first logical operation one of the plurality of keys ~~a particular key~~ provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of ~~associated with~~ the first portion of the data block;

~~means~~ substitution logic for receiving the second bit sequence and for generating a [[second]] third bit sequence ~~based on the output of the first logical operation~~;

[[an]] a first inverse permutation logic for performing , during an initial cryptographic round, an inverse permutation of the first ~~a bit sequence associated with the second~~ portion of the data block and for generating [[an]] a first inverse permuted bit sequence , wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logical operation the [[second]] third bit sequence with the second inverse permuted bit sequence to generate ~~and generating~~ a [[combined]] fourth bit sequence; and

a permutation logic for permuting the ~~combined~~ fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

69. (previously presented) The cryptography engine of claim 68, wherein the first and second logical operations are binary XOR operations.

70. (previously presented) The cryptography engine of claim 68, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

71. (currently amended) The cryptography engine of claim 70, wherein the [[second]] third bit sequence is less than the first bit sequence.

72. (previously presented) The cryptography engine of claim 68, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

73. (currently amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the integrated circuit layout providing information for configuring the cryptographic engine, the integrated circuit layout comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

means for combining via a first logical operation one of the plurality of keys ~~a particular key~~ provided by the key scheduler with a first bit sequence to generate a second bit sequence, wherein the first bit sequence is an expansion of ~~associated with~~ the first portion of the data block;

~~means~~ substitution logic for receiving the second bit sequence and for generating a [[second]] third bit sequence ~~based on the output of the first logical operation~~;

[[an]] a first inverse permutation logic for performing , during an initial cryptographic round, an inverse permutation of the first ~~a bit sequence associated with the second~~ portion of the data block and for generating [[an]] a first inverse permuted bit sequence , wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

means for combining via a second logical operation the [[second]] third bit sequence with the second inverse permuted bit sequence to generate ~~and generating~~ a [[combined]] fourth bit sequence; and

a permutation logic for permuting the ~~combined~~ fourth bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

74. (previously presented) The integrated circuit layout of claim 73, wherein the first and second logical operations are binary XOR operations.

75. (previously presented) The integrated circuit layout of claim 73, wherein the first bit sequence is a bit sequence expanded by an expansion logic.

76. (currently amended) The integrated circuit layout of claim 73, wherein the [[second]] third bit sequence is less than the first bit sequence.

77. (previously presented) The integrated circuit layout of claim 73, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.

78. (currently amended) A cryptography engine for performing cryptographic operations on a data block having a first portion and a second portion, the cryptography engine comprising:

a key scheduler configured to provide a plurality of keys for cryptographic operations;

an expansion logic for expanding ~~a bit sequence associated with~~ the first portion of the data block and for generating a first bit sequence ~~an expanded bit sequence~~ having a first bit size;

a first XOR logic for performing a first XOR operation of a first key provided by the key scheduler and the ~~expanded bit sequence~~ first bit sequence and for generating a ~~first combined~~ second bit sequence;

an Sbox logic for taking the second ~~first combined~~ bit sequence and for generating a [[second]] third bit sequence having a second bit size smaller than the first bit size;

[[an]] a first inverse permutation logic for performing , during an initial cryptographic round, an inverse permutation of the first ~~a bit sequence associated with the second~~ portion of the data block and for generating [[an]] a first inverse permuted bit sequence , wherein the first inverse permuted bit sequence is a first input bit sequence for a subsequent cryptographic round;

a second inverse permutation logic for performing, during an initial cryptographic round, an inverse permutation of the second portion of the data block and for generating a second inverse permuted bit sequence;

a second XOR logic performing a second XOR operation of the [[second]] third bit sequence and the second inverse permuted bit sequence to generate ~~and generating~~ a ~~second combined~~ fourth bit sequence; and

a permutation logic for permuting the fourth ~~second combined~~ bit sequence and generating a permuted bit sequence, wherein the permuted bit sequence is a second input bit sequence for the subsequent cryptographic round.

79. (previously presented) The cryptography engine of claim 78, wherein the data block contains bits 0 to M, the first portion contains bits 0 to N, and the second portion contains bits N+1 to M.